# IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

| | | | |
|---|---|---|---|
| Applicants: | William B. Sweet | Examiner: Jeffrey D. Popham | |
| Serial No.: | 0/930,029 | Art Unit: | 2437/Conf. Num: 3170 |
| Filed: | 8/14/2001 | Docket No.: | 00131-000100000 |
| Title: | METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT | | |

## DECLARATION UNDER 37 C.F.R. § 1.132

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Examiner:

I declare as follows:

1. I am one of the inventors associated with the subject patent application filed on August 14, 2001.

2. At the time the patent application was filed, Viaquo Corporation of San Jose California ("Viaquo") was the sole owner of all rights associated with the application and I served as Chief Executive Officer (CEO) of Viaquo.

3. Viaquo developed cryptographic solutions, key distribution methods and other systems useful for securing data, performing access control and other tasks.

4. At the time the subject patent application was filed, TECSEC, Inc. from Vienna Va. had developed a cryptographic method called constructive key management or CKM. CKM used a combination of different key splits to assemble or 'construct' a working key to either encrypt or decrypt data. In TECSEC parlance, the combinations of key splits were referred to as a user's 'credentials' and managed by a Credential Manager. The CKM method used data encapsulation and multiple layers of encryption to provide selected users access, read, and/or modify rights to a container object and data contained inside. This enabled CKM to provide the selected user access to one container object but not another container object—even if it were inside the accessible container object. Consequently, a user with the proper credentials could not only decrypt and access certain container objects but also could also generate the proper working key and begin to encrypt certain container objects and data.

5. The credentials in CKM were typically assigned to different groups of users according to their roles in an organization and information they processed. A group of users employed in a human resources department might be given the role of "Human Resources" with access to employment records and resumes but not salaries. Users managing employees given the role of "Management" might be able to access detailed salary information as well as the employment records and resumes.

6. CKM could also quickly revoke access to certain information by changing the credentials and re-encrypting the associated information. Once the credentials were changed, even users having the proper role in the organization would not be able to access the newly encrypted information. A user could only decrypt container objects if the user's new set of credentials were updated on their smart cards and re-distributed.

7. Before handing out credentials, TECSEC required an in-person positive identification of each person for authentication purposes. Once authenticated in this manner, the credentials for the authenticated user were stored on a smart card or other storage medium and then safely handed to the particular user. The requirement for a face-to-face authentication in the TECSEC system was driven, in part, by its founder Mr. Ed Scheidt. Mr. Scheidt preferred in-person authentication at the time credentials were distributed to avoid the threats of hackers and the opportunity for them to credential possibly hundreds of "bogus" users in the system. As far as Mr. Scheidt and TECSEC were concerned, electronic management of the credentials over a network, especially the Internet, was not a viable option. Accordingly, the system was kept secure by manually issuing smart cards holding their credentials for CKM and handing them out individually. Likewise it was also important for TECSEC to reissue these credentials in a similar manner. To reissue, TECSEC placed updated credentials on the smart card and then hand-delivered the smart card to the person or through the United States Postal Service (USPS) to an address provided by the authenticated user.

8. Members of Viaquo began working on commercial application of the TECSEC technology as early as 2000. I had personal experience working with TECSEC and TECSEC founder, Mr. Ed Scheidt, at or about this time period. The TECSEC in-person or manual distribution of credentials via a smart card posed problems of scalability and overall

ease of use for commercial applications being developed by our team. Viaquo used the unwieldy and difficult to use TECSEC technology as an opportunity to improve the key distribution method and open up new markets for the CKM technology. Meanwhile, TECSEC continued using their manual in-person authentication in their belief that key distribution over a network was inherently insecure.

9. Over the next many months, Viaquo was able to greatly improve the scalability of the TECSEC solution using intranets and the Internet. Viaquo created a method and system to update credentials over these networks using soft-tokens. Still, TECSEC refused to use the Internet-driven key distribution developed by Viaquo. Mr. Scheidt and TECSEC remained skeptical of using public or private networks to perform key management. TECSEC thought the Viaquo system for key distribution would scale but would result in a lower class of security and therefore much too risky. TECSEC remained focused on face-to-face authentication for each smart card and physical delivery for issuance and re-issuance.

10. I have reviewed United States Patent 6,490,680 to Scheidt ("the Scheidt patent") and it supports my aforementioned account of events and communications.

a. The Scheidt patent appears to only provide for an in-person authentication followed by a manual distribution of a smart card with newly created credentials. On Col. 9, lines 39-55, the Scheidt patent describes that "the card is then given to the user" and "It is preferable that the user is present at this step, or that a method is used to assure the user's identity." The Scheidt patent does teach that the smart card with credentials should be handed over to a person only if they have been properly authenticated in-person. Conversely, the Scheidt patent does not mention here or elsewhere that the credentials can be transmitted over a network or the Internet.

b. Later, the Scheidt patent states that updated credentials may be distributed without in-person authentication by a Credentials Manager but still not over a network or the Internet. The Scheidt patent states that someone other than the Credentials Manager may give the new credentials to a user since the user has already been authenticated previously. (Col. 10, lines 20-23 of the Scheidt patent) Indeed, passwords may be sent over an organizational administrative channel but not over the Internet. (Col. 10, lines 24-26 of the Scheidt patent) Organizational administrative

channels might use inter-office mail pouches, USPS or courier. The organizational administrative channels in the Scheidt patent do not appear to include a network or the Internet. If the Scheidt patent had intended to include a network as part of the distribution then they would have expressly specified this as a possible solution.

11. We declare that all statements made herein are of our own knowledge and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Name: W.B. Sweet Date: May 25, 2009

William B. Sweet